日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　２月２７日

出願番号
Application Number: 特願２００３－０５０２４３

[ST. 10/C]: ［ＪＰ２００３－０５０２４３］

出願人
Applicant(s): 株式会社ルネサステクノロジ

CERTIFIED COPY OF
PRIORITY DOCUMENT

BEST AVAILABLE COPY

２００４年　２月１７日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

【書類名】　特許願
【整理番号】　K03003931A
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/00
【発明者】
【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
【氏名】　水島　永雅
【発明者】
【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
【氏名】　角田　元泰
【発明者】
【住所又は居所】　東京都小平市上水本町五丁目２０番１号　株式会社日立製作所半導体グループ内
【氏名】　片山　国弘
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社日立製作所
【代理人】
【識別番号】　100075096
【弁理士】
【氏名又は名称】　作田　康夫
【先の出願に基づく優先権主張】
【出願番号】　特願2003- 28998
【出願日】　平成15年 2月 6日
【手数料の表示】
【予納台帳番号】　013088
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9902691

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　メモリカード

【特許請求の範囲】

【請求項１】

外部のホスト機器と接続するためのインターフェイスと、

前記アプリケーションプログラムを格納可能で、前記アプリケーションプログラムを実行可能なＩＣカードチップと、

前記アプリケーションプログラムに関係した関係データを格納可能な不揮発性メモリと、

前記インターフェイスと前記ＩＣカードチップと前記不揮発性メモリに接続されたコントローラとを備え、

前記コントローラは、前記ホスト機器から前記インターフェイスで受信された特定コマンドに応答して、前記ＩＣカードチップと前記不揮発性メモリの間の前記関係データの転送を実行して、前記インターフェイスを介した前記ホスト機器への前記関係データの転送を禁止するメモリカード。

【請求項２】

請求項１に記載のメモリカードにおいて、

前記ＩＣカードチップは、前記複数のアプリケーションプログラムを格納及び実行可能で、

前記不揮発性メモリは、複数のブロックに分割され、

前記複数のブロックの各ブロックは、各アプリケーションプログラムに割り当てられ、各関係データを格納可能であるメモリカード。

【請求項３】

請求項２に記載のメモリカードにおいて、

前記不揮発性メモリは、前記アプリケーションプログラムを識別するためのアプリケーションＩＤと、前記不揮発性メモリから前記ＩＣカードチップへの前記関係データの転送のためのオペレーションコードを対応づけて格納する管理領域を有するメモリカード。

【請求項４】

請求項３に記載のメモリカードにおいて、

前記ＩＣカードチップに少なくとも１つのアプリケーションプログラムを格納した場合に、前記ＩＣカードチップに格納されたアプリケーションプログラムに対応する前記不揮発性メモリ内の前記アプリケーションＩＤの変更又は追加又は削除を禁止するロック機能と前記ロック機能を解除するアンロック機能を有するメモリカード。

【請求項５】

請求項３又は４に記載のメモリカードにおいて、

前記コントローラは、前記ＩＣカードからのアプリケーションＩＤと前記不揮発性メモリからのアプリケーションＩＤとを比較し、両者が一致した場合に、前記ＩＣカードチップと前記不揮発性メモリの間の前記関係データの転送を許可するメモリカード。

【請求項６】

請求項１～５の何れかに記載のメモリカードにおいて、

前記関係データは、最初の使用から前記不揮発性メモリに格納されるメモリカード。

【請求項７】

請求項６に記載のメモリカードにおいて、

前記関係データは、前記ＩＣカードチップ内のメモリに格納されることなく、最初の使用から前記不揮発性メモリに格納されるメモリカード。

【請求項８】

請求項１～７の何れかに記載のメモリカードにおいて、

前記特定コマンドに応答した前記関係データの転送の実行及び禁止は、前記不揮発性メモリから前記ＩＣカードチップへの前記アプリケーションプログラムに対応する制御コマンドによって制御されるメモリカード。

【請求項９】

複数のブロックに分割されたメモリと、ＩＣカードチップと、前記メモリ及び前記ＩＣカードリップへのアクセスを制御するコントローラを備えたメモリカードにおいて、

前記メモリの各ブロックは、前記ＩＣカードチップによって実行されるアプリケーションプログラムのために前記アプリケーションプログラムごとに割り当てられ、

前記メモリは、前記ＩＣカードチップから前記コントローラへ指示する処理の内容を前記コントローラから前記ＩＣカードチップへ問い合わせるためのコマンドを記憶可能で、

前記ＩＣカードチップは、当該ＩＣカードチップが実行すべきアプリケーションプログラムのアプリケーションＩＤを前記コントローラへ送出し、

前記コントローラは、前記メモリ内の特定コマンドのうち前記ＩＣカードチップからの前記アプリケーションプログラムＩＤに対応する前記コマンドを特定し、特定された前記コマンドを前記ＩＣカードチップへ送出し、

前記ＩＣカードチップは、前記コントローラからの前記コマンドに応答して、前記処理の内容を前記コントローラへ指示し、

前記コントローラは、前記ＩＣカードチップからの指示に応答して、前記処理を実行するメモリカード。

【請求項１０】

請求項９に記載のメモリカードにおいて、

前記コマンドは、前記メモリのブロックへ書き込むべきデータを前記ＩＣカードチップから前記コントローラへ転送するための第１の転送コマンドと、前記メモリのブロックから読み出されたデータを前記コントローラから前記ＩＣカードチップへ転送するための第２の転送コマンドとを含むメモリカード。

【請求項１１】

請求項１０に記載のメモリカードにおいて、

前記コマンドは、外部のホスト機器からのコマンドと異なるメモリカード。

【請求項１２】

複数のブロックに分割されたメモリと、ＩＣカードチップと、前記メモリ及び前記ＩＣカードチップへのアクセスを制御するコントローラを備えたメモリカードにおいて、

前記コントローラは、外部のホスト機器からの第１のコマンドに応答して、前

記メモリのブロックの利用権を、前記ＩＣカードチップによって実行されるべきアプリケーションプログラムのために前記アプリケーションプログラムごとに割り当て、

前記コントローラは、前記ホスト機器からの第２のコマンドに応答して、前記第１のコマンドに応答した処理を実行可能なアンロック状態から前記第１のコマンドに応答した処理を拒否するロック状態へ遷移するメモリカード。

【請求項１３】

請求項１２に記載のメモリカードにおいて、

前記メモリは、前記ブロックの識別子と前記ブロックの利用権が割り当てられたアプリケーションプログラムの識別子との対応を管理するための管理情報を記憶可能で、

前記コントローラは、前記アンロック状態である場合に、前記管理情報の内容の変更を許可し、

前記コントローラは、前記ロック状態である場合に、前記管理情報の内容の変更を禁止するメモリカード。

【請求項１４】

請求項１２に記載のメモリカードにおいて、

前記メモリは、前記ブロックの識別子と前記ブロックの利用権が割り当てられたアプリケーションプログラムの識別子との対応を管理するための管理情報を記憶可能で、

前記コントローラは、前記ブロックの利用権を前記アプリケーションプログラムのために割り当てる場合に、前記ブロックの識別子に対応する前記アプリケーションプログラムの識別子を前記管理情報に追加するメモリカード。

【請求項１５】

請求項１２に記載のメモリカードにおいて、

前記メモリは、前記第１のコマンドに応答した処理を実行可能か否かを識別するためのフラグを記憶可能で、

前記コントローラは、前記アンロック状態から前記ロック状態へ遷移する場合に、前記フラグの値を変更するメモリカード。

【請求項１６】

請求項１２に記載のメモリカードにおいて、

前記コントローラは、前記ホスト機器からの第３のコマンドに応答して、前記ロック状態から前記アンロック状態へ遷移するメモリカード。

【請求項１７】

請求項１６に記載のメモリカードにおいて、

前記メモリは、前記第３のコマンドに応答した処理を許可するための参照パスワードを記憶可能で、

前記コントローラは、前記ホスト機器から受け取ったパスワードと前記メモリ内の前記参照パスワードとが一致した場合に、前記第３のコマンドに応答して、前記ロック状態から前記アンロック状態へ遷移するメモリカード。

【請求項１８】

請求項１２に記載のメモリカードにおいて、

前記コントローラは、前記ホスト機器からの第４のコマンドに応答して、前記アプリケーションプログラムのために割り当てられた前記ブロックの利用権を解除するメモリカード。

【請求項１９】

請求項１８に記載のメモリカードにおいて、

前記メモリは、前記ブロックの識別子と前記ブロックの利用権が割り当てられたアプリケーションプログラムの識別子との対応を管理するための管理情報を記憶可能で、

前記コントローラは、前記アプリケーションプログラムのために割り当てられた前記ブロックの利用権を解除する場合に、前記ブロックの識別子に対応する前記アプリケーションプログラムの識別子を前記管理情報から削除するメモリカード。

【請求項２０】

請求項１２に記載のメモリカードにおいて、

前記メモリは、前記ホスト機器から受け取ったデータを記憶するための第１のエリアと、前記アプリケーションプログラムのために前記ブロックの利用権が割

り当てられた第２のエリアとを有するメモリカード。

【請求項２１】

請求項２０に記載のメモリカードにおいて、

前記コントローラは、前記メモリの前記第２のエリアへ書き込むべきデータを前記ＩＣカードチップから受信し又は前記第２のエリアから読み出されたデータを前記ＩＣカードチップへ送信するための転送コマンドを前記アプリケーションプログラムごとに生成するメモリカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、セキュリティ機能を搭載した記憶装置及びその記憶装置が挿入可能なホスト機器及びその記憶装置を備えたホスト機器に係り、フラッシュメモリチップとコントローラチップとＩＣカードチップを有するメモリカード等に関する。

【０００２】

【従来の技術】

特許文献１には、ＩＣモジュールと大容量のフラッシュメモリを搭載するメモリカードが記載されている。

【０００３】

特許文献２には、アプリケーションプログラムごとの実行必須条件をＩＣカードに記憶させておき、処理要求があった時に実行必須条件を充足していれば実行可能とし、充足していなければ実効不能とすることが記載されている。

【０００４】

特許文献３には、ＩＣカード内のメモリ領域のうち、銀行のために領域Ａが、病院のために領域Ｂが、それぞれ割り付けられていることが記載されている。

【０００５】

【特許文献１】特開平10-198776号公報

【特許文献２】特開2000-66882号公報

【特許文献３】特開平6-222980号公報

【０００６】

【発明が解決しようとする課題】

しかし、何れの従来技術も、ＩＣカードのアプリケーションプログラム（アプレット）ごとに、分割された記憶エリアを割り当てることまでは記載されていない。よって、従来技術では、各アプリケーションプログラムが互いのメモリ内のデータを不正に侵害することが懸念される。

【０００７】

本発明の目的は、特定のアプリケーションプログラムに係る処理を実行する場合に、特定のアプリケーションプログラムに関係するデータをメモリ装置内部で処理することにより、特定のアプリケーションプログラムに係る処理の安全性を向上するメモリ装置を提供することである。

【０００８】

本発明の目的は、ＩＣカードチップのアプリケーションプログラム間のデータ干渉、即ち、あるアプリケーションプログラムに割り当てられたメモリが他のアプレットにもアクセスされてデータが侵害されることを抑制できる記憶媒体を提供することである。

【０００９】

【課題を解決するための手段】

本発明は、コントローラが、ホスト機器からインターフェイスで（例えば、外部端子）受信された特定コマンドに応答して、ＩＣカードチップと不揮発性メモリ（例えば、フラッシュメモリの間のアプリケーションプログラムに関係した関係データ（例えば、アプリケーションプログラムによって処理されるべきデータ）の転送を実行して、インターフェイスを介したホスト機器への関係データの転送を禁止する。

【００１０】

また、本発明は、メモリを複数のブロックに分割し、ブロックの使用権をＩＣカードチップのアプリケーションプログラムごとに割り当てた。つまり、メモリが、ホスト機器からのデータを記憶するための第１の記憶エリア（例えば、ノーマルデータエリア）とＩＣカードチップからのデータを記憶するための第２の記

憶エリア（例えば、セキュアデータエリア）を有し、さらに、第２の記憶エリアが複数のブロックに分割され、さらに各ブロックがアプリケーションプログラムごとに割り当てられる。

【００１１】

また、本発明は、ホスト機器からコマンドによって、ブロックの使用権の割り当て、割り当て解除、割り当て及び解除の禁止、割り当て及び解除の禁止の解除を行うようにした。つまり、本発明は、ホスト機器からの第１のコマンド（例えば、アプレット登録コマンド）に応答してメモリのブロックの利用権をアプリケーションプログラムごとに割り当て、ホスト機器からの第２のコマンド（例えば、管理テーブルロックコマンド）に応答してアンロック状態からロック状態へ遷移する。さらに、ホスト機器からの第３のコマンド（例えば、管理テーブルアンロックコマンド）に応答してロック状態からアンロック状態へ遷移し、ホスト機器からの第４のコマンド（例えば、アプレット登録解除コマンド）に応答してアプリケーションプログラムのために割り当てられたブロックの利用権を解除する。

【００１２】

【発明の実施の形態】

以下、本発明の一実施形態について説明する。

【００１３】

図１は、本発明を適用したＭｕｌｔｉＭｅｄｉａＣａｒｄ（ＭｕｌｔｉＭｅｄｉａＣａｒｄはＩｎｆｉｎｅｏｎＴｅｃｈｎｏｌｏｇｉｅｓＡＧの登録商標である。以下、「ＭＭＣ」と略記する。）の内部構成図を簡単に表したものである。ＭＭＣ１１０は、ＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠するのが好ましい。ＭＭＣ１１０は、外部に接続したホスト機器１６０がＭｕｌｔｉＭｅｄｉａＣａｒｄのプロトコル仕様に準拠したメモリカードコマンドを発行することによって、ファイルデータを読み書きすることができるストレージ機能や、機密データ保護や個人認証などに必要な暗号演算をおこなうことができるセキュリティ処理機能を有する。ホスト機器１６０は、例えば、携帯電話、携帯情報端末（ＰＤＡ）、パーソナルコンピュータ、音楽再生（及び録音）装置、カメラ、ビデオカメラ

、自動預金預払器、街角端末、決済端末等が該当する。ＭＭＣ１１０は、ＭＭＣ外部端子１４０、コントローラチップ１２０、フラッシュメモリチップ１３０、ＩＣカードチップ１５０を持つ。フラッシュメモリチップ１３０は、不揮発性の半導体メモリを記憶媒体とする大容量（例えば、６４メガバイト）のメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。ＭＭＣ外部端子１４０は７つの端子から構成され、外部のホスト機器１６０と情報交換するために、電源供給端子、クロック入力端子、コマンド入出力端子、データ入出力端子、グランド端子を含む。コントローラチップ１２０は、ＭＭＣ１１０内部の他の構成要素（ＭＭＣ外部端子１４０、フラッシュメモリチップ１３０、ＩＣカードチップ１５０）と接続されており、これらを制御するマイコンチップである。ＩＣカードチップ１５０は、ＩＣカードのプラスチック基板中に埋め込むためのマイコンチップであり、その外部端子、電気信号プロトコル、コマンドはＩＳＯ／ＩＥＣ７８１６規格に準拠している。ＩＣカードチップ１５０の外部端子には、電源供給端子、クロック入力端子、リセット入力端子、Ｉ／Ｏ入出力端子、グランド端子がある。ＩＣカードチップ１５０の外部端子は、グランド端子を除いて、電源供給端子、クロック入力端子、リセット入力端子、Ｉ／Ｏ入出力端子がコントローラチップ１２０に接続されている。コントローラチップ１２０は、ＩＣカードチップ１５０の外部端子からＩＣカードチップ１５０にＩＣカードコマンドを発行することによって、外部のホスト機器１６０から要求されたセキュリティ処理に必要な演算をおこなう。ＩＣカードチップ１５０は、演算処理を行うためのＣＰＵ１５１と、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１５２とを備える。一方、フラッシュメモリチップ１３０には、記憶素子を備えるが、マイコンは存在しない。

【００１４】

セキュリティ処理は、例えば、ＩＣカードチップ１５０内のＥＥＰＲＯＭ１５２にデータが書き込まれるとき、又は、ＥＥＰＲＯＭ１５２からデータが読み出されるときにＣＰＵ１５１により実行される。セキュリティ処理の詳細な内容は、ＥＥＰＲＯＭ１５２内に格納されたプログラムコードによって記述されている

。多種多様なセキュリティ処理に適用できるように、そのプログラムコードは機能的に異なる複数のモジュールとして構成されている。ＣＰＵ１５１は必要に応じてセキュリティ処理に使用するモジュールを切り替えることができる。以下、このモジュール単位をアプレットと呼ぶ。例えば、ＥＥＰＲＯＭ１５２は、アプレットＡ１５３とアプレットＢ１５４とを格納する。ＩＣカード内の各アプレットはそれぞれ、自身のアプリケーション識別子（以下、ＡＩＤ（Ａｐｐｌｉｃａｔｉｏｎ ＩＤｅｎｔｉｆｉｅｒ）と呼ぶ。）を所有する。図１において、アプレットＡ１５３のＡＩＤは１５５として、アプレットＢ１５４のＡＩＤは１５６として示されている。これらのＡＩＤは、ＩＣカードのアプリケーションプログラムを識別するために、国際的にユニークに割り振られた値であることが好ましい。国際的に流通するＡＩＤの付番方法は、国際規格としてＩＳＯ／ＩＥＣ７８１６－５で規定されている。ＥＥＰＲＯＭ１５２の記憶容量は例えば６４キロバイトであり、フラッシュメモリチップ１３０の記憶容量より小さい。但し、本発明を実施する上で、ＥＥＰＲＯＭ１５２の記憶容量は、フラッシュメモリチップ１３０の記憶容量と同じでもよいし、大きくてもよい。

【００１５】

ＩＣカードチップ１５０には、セキュリティ評価基準の国際標準であるＩＳＯ／ＩＥＣ１５４０８の評価・認証機関によって認証済みである製品を利用する。一般に、セキュリティ処理をおこなう機能を持つＩＣカードを実際の電子決済サービスなどで利用する場合、そのＩＣカードはＩＳＯ／ＩＥＣ１５４０８の評価・認証機関による評価と認定を受ける必要がある。ＭＭＣにセキュリティ処理をおこなう機能を追加することによってＭＭＣ１１０を実現し、それを実際の電子決済サービスなどで利用する場合、ＭＭＣ１１０も同様にＩＳＯ／ＩＥＣ１５４０８の評価・認証機関による評価と認定を受ける必要がある。ＭＭＣ１１０は、評価・認証機関によって認証済みのＩＣカードチップ１５０を内蔵し、そのＩＣカードチップ１５０を利用してセキュリティ処理をおこなう構造を持つことにより、セキュリティ処理機能を得る。したがって、ＭＭＣ１１０はＩＳＯ／ＩＥＣ１５４０８に基づくセキュリティ評価基準を容易に満足することができ、ＭＭＣにセキュリティ処理機能を追加するための開発期間を短縮することができる。

【００１６】

ＭＭＣ１１０は、ＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した外部インタフェースを持つのが好ましい。ＭＭＣ１１０は、一種類の外部インタフェースを通じて、ＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した標準メモリカードコマンドに加えて、セキュリティ処理を実行するコマンド（以下、セキュアライトコマンドと呼ぶ。）を受け付ける。セキュアライトコマンドは入力データを伴う。コントローラチップ１２０は、ＭＭＣ１１０が受信したコマンドが標準メモリカードコマンドであるか、セキュアライトコマンドであるかによって、アクセスすべきチップを選択し、コマンド処理を分配する機能を持つ。標準メモリカードコマンドを受信したならば、フラッシュメモリチップ１３０を選択し、これにフラッシュメモリコマンドを発行してホストデータを読み書きできる。また、セキュアライトコマンドを受信したならば、ＩＣカードチップ１５０を選択し、これにＩＣカードコマンドを発行してセキュリティ処理を実行することができる。ここで発行されるＩＣカードコマンドは、セキュアライトコマンドによって入力されるデータ（以下、セキュアライトデータと呼ぶ。）の中に埋め込まれている。ＩＣカードチップ１５０はこのコマンドに応じてＩＣカードレスポンスを返すが、コントローラチップ１２０はそれをキャッシュする。さらに、ＭＭＣ１１０は、一種類の外部インタフェースを通じて、セキュリティ処理の結果を読み出すコマンド（以下、セキュアリードコマンドと呼ぶ。）も受け付ける。セキュアリードコマンドは出力データを伴う。セキュアリードコマンドを受信したならば、キャッシュしておいたＩＣカードレスポンスを含むデータ（以下、セキュアリードデータと呼ぶ。）を出力する。

【００１７】

図２は、本発明を適用したＭＭＣ１１０の動作を概念的に示すフローチャートである。以下、図２を参照しながらその動作を説明する。ホスト機器１６０はＭＭＣ１１０にセキュアライトコマンドを送信すると（２０１）、コントローラチップ１２０はＩＣカードチップ１５０にＩＣカードコマンドを送信する（２０２）。ＩＣカードチップ１５０はＩＣカードコマンドを受信すると（２０３）、そのとき選択されているアプレットのＡＩＤを含むＩＣカードレスポンスをコント

ローラチップ１２０に返信する（２０４）。コントローラチップ１２０がそのＩＣカードレスポンスを受信したらフラッシュメモリチップ１３０にリードコマンドを送信する（２０５）。これにより、フラッシュメモリチップ１３０はＡＩＤのリスト（事前に書き込んで置くものとする。）を読み出して（２０６）、コントローラチップ１２０に出力する。コントローラチップ１２０はそのリストから、ＩＣカードチップ１５０からのＡＩＤに一致するものがあるか検索する（２０７）。一致するＡＩＤを検出できないならば、ホスト機器１６０からセキュアリードコマンドを受けてＩＣカードレスポンスをセキュアリードデータとして送信し（２１９）、ホスト機器１６０がそれを受信する（２２０）。一方、ステップ２０７で、ＡＩＤを検出したならば、ＩＣカードレスポンスをホスト機器１６０に出力するのを禁止し、ＩＣカードチップ１５０にＩＣカードコマンドを送信する（２０８）。ＩＣカードチップ１５０がこのＩＣカードコマンドを受信すると（２０９）、選択されているアプレットは、ＩＣカードチップ１５０とフラッシュメモリチップ１３０との間でデータを転送するため、データ転送方向に応じたＩＣカードレスポンスを作成する。ＩＣカードからフラッシュへ転送したいならば、フラッシュメモリにライトするデータとそのアドレスを含んだＩＣカードレスポンスを作成して返信する（２１１）。フラッシュからＩＣカードへ転送したいならば、フラッシュメモリからリードしたいアドレスを含んだＩＣカードレスポンスを作成して返信する（２１４）。ステップ２１１のあと、コントローラチップ１２０はフラッシュメモリチップ１３０にライトコマンドを送信する（２１２）。これに対し、フラッシュメモリチップ１３０は指定されたアドレスにデータを書き込む（２１３）。これにより、ＩＣカードからフラッシュへのデータ転送が完了する。一方、ステップ２１４のあと、コントローラチップ１２０はフラッシュメモリチップ１３０にリードコマンドを送信する（２１５）。これに対し、フラッシュメモリチップ１３０は指定されたアドレスからデータを読出し（２１６）、コントローラチップ１２０に出力する。コントローラチップ１２０は。そのリードデータをＩＣカードコマンドによってＩＣカードチップ１５０に送信し（２１７）、ＩＣカードチップ１５０がこれを受信する（２１８）。これにより、フラッシュからＩＣカードへのデータ転送が完了する。　図６は、セキュア

ライトデータおよびセキュアリードデータのフォーマットの一例を示したものである。このフォーマットは、実行するセキュリティ処理の内容が１つのＩＣカードコマンドで表現でき、セキュリティ処理の結果が１つのＩＣカードレスポンスで表現できる場合に適用することが好ましい。上述の通り、ＩＣカードチップ１５０に送信するＩＣカードコマンド、ＩＣカードチップ１５０から受信するＩＣカードレスポンスはともにＩＳＯ／ＩＥＣ７８１６－４規格に従う。本規格によれば、ＩＣカードコマンドの構成は、４バイトのヘッダ（クラスバイトＣＬＡ、命令バイトＩＮＳ、パラメータバイトＰ１とＰ２）が必須であり、必要に応じて、入力データ長指示バイトＬｃ、入力データフィールドＤａｔａＩｎ、出力データ長指示バイトＬｅが後に続く。また、ＩＣカードレスポンスの構成は、２バイトのステータスＳＷ１とＳＷ２が必須であり、必要に応じて、出力データフィールドＤａｔａＯｕｔがその前に置かれる。本フォーマットにおけるセキュアライトデータ６０１は、ＩＣカードコマンド６０２の前にＩＣカードコマンド長Ｌｃａ６０４を付け、さらにＩＣカードコマンド６０２の後にダミーデータ６０５をパディングしたものである。Ｌｃａ６０４の値はＩＣカードコマンド６０２の各構成要素の長さを合計した値である。一方、セキュアリードデータ６１１は、ＩＣカードレスポンス６１２の前にＩＣカードレスポンス長Ｌｒａ６１４を付け、さらにＩＣカードレスポンス６１２の後にダミーデータ６１５をパディングしたものである。Ｌｒａ６１４の値はＩＣカードレスポンス６１２の各構成要素の長さを合計した値である。なお、この図では、ＩＣカードコマンドにＬｃ、ＤａｔａＩｎ、Ｌｅが含まれ、ＩＣカードレスポンスにＤａｔａＯｕｔが含まれる場合のフォーマット例を表している。ＭＭＣ１１０に対する標準メモリカードコマンドに含まれるデータリード／ライトコマンドの仕様では、リード／ライトアクセスするデータを固定長のブロック単位で処理することが基本となっている。よって、セキュアライトデータ６０１やセキュアリードデータ６１１のサイズも、ＭＭＣ１１０の標準メモリカードコマンドの仕様に準拠したブロックサイズに一致させることが好ましい。ダミーデータ６０５、６１５は、セキュアライトデータ６０１やセキュアリードデータ６１１のサイズをブロックサイズに一致させるために適用される。ブロックサイズとして採用する値は、一般の小型メモリカード

が論理ファイルシステムに採用しているＦＡＴ方式におけるセクタサイズ（５１２バイト）が望ましい。パディングするダミーデータ６０５、６１５は全てゼロでもよいし、乱数でもよいし、コントローラチップ１２０やホスト機器１６０がデータエラーを検出したり訂正するためのチェックサムでもよい。Ｌｃａ６０４の値はコントローラチップ１２０がセキュアライトデータ６０１からダミーデータ６０５を除去してＩＣカードコマンド６０２を抽出するために使用し、Ｌｒａ６１４の値はホスト機器１６０がセキュアリードデータ６１１からダミーデータ６１５を除去してＩＣカードレスポンス６１２を抽出するために使用する。

【００１８】

コントローラチップ１２０は、電源供給端子、クロック入力端子を通して、ＩＣカードチップ１５０への電源供給、クロック供給を制御する。ホスト機器１６０からセキュリティ処理を要求されないときには、ＩＣカードチップ１５０への電源供給やクロック供給を停止させることができ、ＭＭＣ１１０の電力消費を削減することができる。

【００１９】

電源供給されていないＩＣカードチップ１５０を、ＩＣカードコマンドを受信できる状態にするには、まず、ＩＣカードチップ１５０に電源供給を開始し、リセット処理を施すことが必要である。コントローラチップ１２０は、ＭＭＣ１１０がホスト機器１６０からセキュアライトコマンドを受信したのを契機に、電源供給端子を通してＩＣカードチップ１５０への電源供給を開始する機能を持つ。また、コントローラチップ１２０は、ＭＭＣ１１０がホスト機器１６０からセキュアライトコマンドを受信したのを契機に、リセット入力端子を通してＩＣカードチップ１５０のリセット処理をおこなう機能を持つ。コントローラチップ１２０は、セキュアライトコマンドを受信するまでＩＣカードチップ１５０への電源供給を停止させておくことができる。したがって、ＭＭＣ１１０の電力消費を削減することができる。

【００２０】

コントローラチップ１２０は、ＩＣカードチップ１５０のクロック入力端子を通してＩＣカードチップ１５０に供給するクロック信号をＭＭＣ１１０内部で発

生し、その周波数、供給開始タイミング、供給停止タイミングを制御する機能を持つ。ＭＭＣ外部端子１４０のクロック入力端子のクロック信号と無関係にすることができるため、ホスト機器１６０によるタイミング解析、電力差分解析、故障利用解析と呼ばれる攻撃法に対してセキュリティが向上する。

【００２１】

フラッシュメモリチップ１３０は、ノーマルデータエリア１３１と管理エリア１３２とセキュアデータエリア１３３とを含む。

【００２２】

ノーマルデータエリア１３１は、セクタ単位に論理アドレスがマッピングされている領域であり、ホスト機器１６０が標準メモリカードコマンドを使用することにより指定した論理アドレスにデータを読み書きできる領域である。

【００２３】

セキュアデータエリア１３３は、ＩＣカードチップ１５０内のＥＥＰＲＯＭ１５２に格納されたアプレット（例えば、１５３や１５４）をＣＰＵ１５１が実行する際に（すなわち、セキュリティ処理を実行する際に）、扱うデータを格納することができる領域である。セキュアデータエリア１３３は複数のブロックに分割されている。これをセキュアデータブロックと呼ぶ。例えば、セキュアデータエリア１３３は４つのセキュアデータブロック１３３ａ、１３３ｂ、１３３ｃ、１３３ｄで構成される。セキュアデータブロックは、コントローラチップ１２０がアプレットごとにその利用権を割り当てることができる単位である。例えば、アプレットＡ１５３はセキュアデータブロックｃ１３３ｃの利用権を持ち、アプレットＢ１５４はセキュアデータブロックａ１３３ａの利用権を持つ。また、各セキュアデータブロックは複数の固定長データレコードに分割されている。例えば、１レコードのサイズは１２８バイトであり、１つのセキュアデータブロック当たり８１９２個のレコードで構成される。このとき、１つのセキュアデータブロックのサイズが１メガバイトとなり、セキュアデータエリア１３３の容量は４メガバイトとなる。したがって、ＥＥＰＲＯＭ１５２に格納されたアプレットは、セキュアデータエリア１３３に格納されたデータにアクセスすることによって、ＥＥＰＲＯＭ１５２の容量以上の不揮発データを利用できる。例えば、ＩＣカ

ードチップ１５０内のアプレットＡ１５３が電子決済に関するセキュリティ処理のためのプログラムである場合、決済ログ（支払金額や日時など）をセキュアデータエリア１３３に格納することにより、ＥＥＰＲＯＭ１５２のみを利用するよりも多くの決済ログが保存でき、ユーザの利便性が高くなる。ＩＣカードチップ１５０からセキュアデータエリア１３３へのアクセス（ライトやリード）は、ＩＣカードチップ１５０からの要求に基づいてコントローラチップ１２０が実行するが、その要求の発生条件はＩＣカードアプレットの任意である。例えば、ＥＥＰＲＯＭ１５２の容量が何らかのしきい値以下になった（ゆえにカード外部に記録せざるを得ない）こと、ＩＣカードチップ内のデータが何らかの保護基準に満たない（ゆえにカード外部に記録しても問題ない）こと、ＥＥＰＲＯＭ１５２の中に所望のデータが見つからない（ゆえにカード外部から読み込む）こと、などが挙げられる。ＩＣカードチップ１５０からセキュアデータエリア１３３へのアクセスの詳細な手順については後に述べる。

【００２４】

一方、管理エリア１３２は、コントローラチップ１２０がセキュアデータエリア１３３を管理するための情報を格納する領域である。コントローラチップ１２０は、ＭＭＣ１１０がホスト機器１６０からセキュアライトコマンドを受信したことを契機に、この領域に情報を格納したり、削除したりする。そのコマンドについては後述する。管理エリア１３２は、ロックフラグ１３４とパスワードエリア１３５と管理テーブル１３６とを含む。

【００２５】

管理テーブル１３６は、セキュアデータエリア１３３を構成している各セキュアデータブロックの利用権を持つアプレットを登録するための領域である。アプレットを識別するために、この領域にＡＩＤを格納することによってアプレットを登録することが望ましい。ＡＩＤを利用することにより、セキュアデータエリア１３３を使用するアプレットを確実に識別することができる。コントローラチップ１２０は、ＡＩＤ１３７に同一のＡＩＤを複数格納することを禁止する。管理テーブル１３６のブロックの欄は、セキュアデータブロックを識別するためのブロック識別子としてブロックの先頭アドレス値を登録する。但し、先頭アドレ

ス値の代わりにMMC内でユニークな番号をブロック識別子として登録してもよい。尚、管理テーブル１３６の代わりに、各セキュアデータブロック内に直接にＡＩＤを登録）してもよい。

【００２６】

管理テーブル１３６には、ＡＩＤ１３７だけでなく、アプレットごとに転送コマンドコード１３８を格納することができる。この転送コマンドコード１３８は、コントローラチップ１２０がセキュアデータブロックの利用権を、アプレットのために割り当てる時に、コントローラチップ１２０によって生成されるのは好ましい。転送コマンドコードとは、“ライト転送コマンド”および“リード転送コマンド”それぞれのコマンドＡＰＤＵ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ Ｄａｔａ Ｕｎｉｔ）のＣＬＡバイトとＩＮＳバイトに設定する２バイト×２個の値である。ここで、“ライト転送コマンド”および”リード転送コマンド”とは、セキュアデータエリア１３３にレコードデータをライトする前、あるいはそこからレコードデータをリードした後に、コントローラチップ１２０とＩＣカードチップ１５０との間でそのレコードデータを転送するために、コントローラチップ１２０がＩＣカードチップ１５０に対して発行するＩＣカードコマンド形式のコマンドである。特に、コントローラチップ１２０へレコードデータを送り出すためのコマンドをライト転送コマンドと呼び、ＩＣカードチップ１５０へレコードデータを送り込むためのコマンドをリード転送コマンドと呼ぶ。これらのコマンドの詳細な説明は後述する。セキュアデータエリア１３３の利用権を持つアプレット（１５３や１５４）には、ライト／リード転送コマンドを受信した際にレコードデータを扱う処理プログラムが記述されている。転送コマンドコード１３８はアプレットごとに個別に決められるようになっている。もし、転送コマンドコードが全てのアプレットに共通の固定値であるならば、ホスト機器１６０からのセキュアライトデータに含まれるアプレット特有のコマンドとライト／リード転送コマンドとの間でコーディングの競合が発生する可能性がある。本発明によれば、このようなコーディング競合を防ぐことができる。なお、転送コマンドコード１３８のうちＩＮＳコードに関しては、伝送プロトコルの都合上ＩＳＯ／ＩＥＣ７８１６－３に準拠していなければならない。

【００２７】

ロックフラグ１３４は、管理テーブル１３６に格納された登録情報の変更の可否を示す１バイトのデータを格納する領域である。この領域にＦＦｈを設定することで管理テーブル１３６の情報の変更が禁止状態（ロック状態）であることを示す。また、００ｈを設定することで管理テーブル１３６の情報の変更が許可状態（アンロック状態）であることを示す。

【００２８】

パスワードエリア１３５は、管理テーブル１３６の情報をアンロック状態にするための２５５バイトのパスワードの参照値を格納しておく領域である。管理テーブル１３６の情報をロックする時には必ず、ホスト機器１６０からセキュアライトコマンドにより、２５５バイトのパスワード参照をこの領域に設定する。管理テーブル１３６の情報をアンロック状態にする場合は、ホスト機器１６０からセキュアライトコマンドにより、ロック時に設定したパスワード参照と同じパスワードを入力する必要がある。入力したパスワードとパスワード参照との一致によって、管理テーブル１３６の情報の変更をアンロックすることができる。

【００２９】

管理エリア１３２は、ホスト機器１６０が不正にアクセスしてセキュリティ処理を解析することができないように、コントローラチップ１２０により物理的にアクセス制限がかけられている。つまり、管理エリア１３２はコントローラチップ１２０による論理アドレスが割り振られていないため、ホスト機器１６０が直接データを読み書きできない。したがって、ＭＭＣ１１０のセキュリティ処理の信頼性や安全性が向上する。

【００３０】

以下、図３を参照しながら、セキュアデータエリア１３３に対するレコードデータのライト／リードアクセスにおいて用いられるライト／リード転送コマンドのコマンドＡＰＤＵとレスポンスＡＰＤＵについて詳細に述べる。

【００３１】

図２ａは、ＩＣカードチップ１５０が出力するレスポンスＡＰＤＵを示している。このレスポンスＡＰＤＵ３００に含まれるＤａｔａＯｕｔ３０４の先頭２バ

イト（以下、先頭から順に第１制御バイト３０１、第２制御バイト３０２と呼ぶ。）、およびＳＷ１バイト３０５とＳＷ２バイト３０６に特別な値を設定することにより、ＩＣカードチップ１５０はコントローラチップ１２０にセキュアデータエリア１３３に対するアクセス要求を通知することができる。なお、後続出力データ３０３（ＤａｔａＯｕｔ３０４のうち第１制御バイト３０１と第２制御バイト３０２を除いた部分）は、アクセス要求に必要な情報を送信するために使用される。

【００３２】

ＩＣカードチップ１５０は、コントローラチップ１２０に対してセキュアデータエリア１３３へアクセスすることを要求するため、ＳＷ１バイト３０５とＳＷ２バイト３０６に９０ＦＦｈという専用のステータス値を設定しなければならない。コントローラチップ１２０は、ＩＣカードチップ１５０が出力するレスポンスＡＰＤＵを常に監視し、ＳＷ１バイト３０５とＳＷ２バイト３０６の値が９０ＦＦｈであることを検出したら、その前方にあるＤａｔａＯｕｔ３０４の第１制御バイト３０１、第２制御バイト３０２第１制御バイト第２制御バイトを調査し、要求されたアクセスの内容などを認知する。一方、９０ＦＦｈでなかった場合は、このレスポンスＡＰＤＵを含むセキュアリードデータをホスト機器１６０に出力する。ただし、ＳＷ１バイト３０５とＳＷ２バイト３０６の値が９０ＦＦｈであっても、条件によって、そのままホスト機器１６０に出力されることがある。その詳細は後述する。

【００３３】

コントローラチップ１２０は、セキュアデータエリア１３３へのアクセスを開始するとき、ＩＣカードチップ１５０上で選択されているアプレットが何であるかによって、１３３ａ～１３３ｄの中からアクティブにするセキュアデータブロックを選択する。アクセスすべきセキュアデータブロックの選択は、ＩＣカードチップ１５０からアクセス開始要求が発生した直後におこなう。アクセス開始要求のためにＤａｔａＯｕｔ３０４に設定するデータの仕様を以下に示す。第１制御バイト３０１の上位４ビットには、０００１を設定する。第１制御バイト３０１の下位４ビットには、アクセスモードを示すコードを設定する。ここで指定可

能なアクセスモードには、レコードデータのライト、レコードデータのリードの２種類がある。０００１というコードはレコードデータのライト、００１０というコードはレコードデータのリードである。その他のコードは無効である。また、後続出力データ３０３には、ＩＣカードチップ１５０上で選択されているアプレットのＡＩＤを設定する。例えば、アプレットＡ１５３が選択されているならばＡＩＤ１５５を、アプレットＢ１５４が選択されているならばＡＩＤ１５６を設定する。第２制御バイト３０２には、そのＡＩＤの長さを設定する。

【００３４】

コントローラチップ１２０は、第１制御バイトの上位４ビットが０００１ならば、後続出力データ３０３に含まれるＡＩＤで管理テーブル１３６内の全てのＡＩＤ１３７を検索し、アクティブにすべきセキュアデータブロックを決定する。一致するＡＩＤが見つからなかった場合は、このレスポンスＡＰＤＵを含むセキュアリードデータをホスト機器１６０に出力する。ＡＩＤを検出し、それに対応するセキュアデータブロックが判明した後、コントローラチップ１２０は、第１制御バイトの下位４ビットが０００１ならばライト、００１０ならばリードのアクセスを開始すると認識する。第１制御バイトの下位４ビットがそれ以外の場合は、このレスポンスＡＰＤＵを含むセキュアリードデータをホスト機器１６０に出力する。

【００３５】

コントローラチップ１２０がアクセスモード（ライトまたはリード）を認知した後、そのモードに応じてライト／リード転送コマンドを発行することによって、アクティブなセキュアデータブロック対してライトすべきレコードデータ、またはリードしたレコードデータをＩＣカードチップ１５０とコントローラチップ１２０との間で転送することができる。図３ｂと図３ｃはライト／リード転送コマンドのコマンドＡＰＤＵを示したものである。図３ｂはコントローラチップ１２０からＩＣカードチップ１５０への転送データがない場合、図３ｃは転送データがある場合を示している。前述のように、ライト／リード転送コマンドのコマンドＡＰＤＵ３１０（または３２０）のＣＬＡバイト３１４（または３２６）とＩＮＳコード３１５（または３２７）にはあらかじめアプレットごとに登録され

たものを設定する。そのため、管理テーブル１３６から２バイト×２個の転送コマンドコード１３８を読み出す。

【００３６】

ライト／リード転送コマンドのコマンドＡＰＤＵ３１０（または３２０）では、直前のアクセスの結果をＩＣカードチップ１５０に通知するため、Ｐ１バイト３１６（または３２８）とＰ２バイト３１７（または３２９）に特殊な値を設定する。０００００ｈは直前のアクセスにエラーがないことを意味する。８０ＸＸｈは直前のアクセスにエラーが発生したことを意味する。なお、ＸＸはエラー内容を示す１６進コードである。エラーの場合、アクティブなセキュアデータブロックへのデータアクセスは実行されない。よって、セキュアデータブロックのレコードデータの内容も変化しない。

【００３７】

ＩＣカードチップ１５０は、ライト／リード転送コマンドのレスポンスＡＰＤＵ３００における後続出力データ３０３を用いて、ライトしたいレコード番号とレコードデータ、またはリードしたいレコード番号をコントローラチップ１２０に送信する。ライトモードでは、指定レコード番号（４バイト）とライトデータ（１２８バイト）の連結データを設定し、リードモードでは、指定レコード番号（４バイト）を設定する。このように、後続出力データ３０３の長さはアクセスモードによって変わるので、ライト／リード転送コマンドのコマンドＡＰＤＵのＬｅバイト３１３（または３２５）には、アクセスモードに応じた値を設定する必要がある。ライトモードでは、後続出力データ３０３の長さが８４ｈとなるのでＤａｔａＯｕｔ３０４の長さは８６ｈとなる。よって、Ｌｅバイト３１３（または３２５）には８６ｈを設定する。リードモードでは、後続出力データ３０３の長さが０４ｈとなるのでＤａｔａＯｕｔ３０４の長さは０６ｈとなる。よって、Ｌｅバイト３１３（または３２５）には０６ｈを設定する。

【００３８】

アクセス開始直後の（つまり、最初に発行される）ライト／リード転送コマンドのコマンドＡＰＤＵは、図３ｂの形式となる。そのとき、Ｐ１バイト３１６とＰ２バイト３１７には、０００００ｈを設定する。Ｌｅバイト３１３には、ライト

モードの場合８６ｈを、リードモードの場合０６ｈを設定する。

【００３９】

ライト／リード転送コマンドのレスポンスＡＰＤＵは、図３ａの形式をとる。ＩＣカードチップ１５０上で選択されているアプレットは、レスポンスＡＰＤＵ３００を利用してアクティブなセキュアデータブロックに対するアクセス（ライト／リード）をコントローラチップ１２０に要求することができる。以下、これをアクセス実行要求と呼ぶ。第１制御バイト３０１と第２制御バイト３０２に設定するデータの仕様を以下に示す。第１制御バイト３０１の上位４ビットには、００１０を設定する。第１制御バイト３０１の下位４ビットには、要求するアクセスを示すコードを設定する。０００１というコードはレコードデータのライト、００１０というコードはレコードデータのリードである。その他のコードは無効である。このコードが表すアクセスモードは、コントローラチップ１２０が認めるアクセスモードに一致していなければならない。また、その第２制御バイト３０２によって、次回のアクセスモード（ライト／リード）の要求をおこなうことができる。コントローラチップ１２０はこれを参照して、自身が認めるアクセスモードをスイッチする。

【００４０】

コントローラチップ１２０は、第１制御バイト３０１の上位４ビットが００１０ならば、アクティブなセキュアデータブロックに対して、指定されたレコード番号のデータをライト／リードする。ライト／リード処理が正常終了した場合（アクセス結果３１２（または３２２）の値が０００００ｈ）、第２制御バイト３０２が０１ｈならば自身が認めるアクセスモードをライトモードにスイッチ、０２ｈならばリードモードにスイッチする。ライト／リード処理に何らかのエラーがあった場合（アクセス結果３１２（または３２２）の値が８０ＸＸｈ）、自身が認めるアクセスモードをスイッチせずにエラーが起きた時点のものを維持する。

【００４１】

コントローラチップ１２０が２回目以降に発行するライト／リード転送コマンドのコマンドＡＰＤＵは、直前のアクセスの結果やアクセスモードの状態遷移によって、図３ｂの形式になったり、図３ｃの形式になったりする。またＬｅ３１

３（または３２５）の値も変わる。その詳細を以下に示す。

【００４２】

直前のライトアクセスが正常で次回もライトモードのとき、図３ｂの形式であり、アクセス結果３１２の値が０００００ｈで、Ｌｅ３１３の値は８６ｈである。

【００４３】

直前のライトアクセスが正常で次回がリードモードのとき、図３ｂの形式であり、アクセス結果３１２の値が０００００ｈで、Ｌｅ３１３の値は０６ｈである。

【００４４】

直前のリードアクセスが正常で次回もリードモードのとき、図３ｃの形式であり、アクセス結果３２２の値が０００００ｈで、Ｌｃ３２３の値は８０ｈで、ＤａｔａＩｎ３２４にはリードしたレコードデータが設定され、Ｌｅ３２５の値は０６ｈである。

【００４５】

直前のリードアクセスが正常で次回がライトモードのとき、図３ｃの形式であり、アクセス結果３２２の値が０００００ｈで、Ｌｃ３２３の値は８０ｈで、ＤａｔａＩｎ３２４にはリードしたレコードデータが設定され、Ｌｅ３２５の値は８６ｈである。

【００４６】

直前のライトアクセスがエラーのとき、図３ｂの形式であり、アクセス結果３１２の値が８０ＸＸｈで、Ｌｅ３１３の値は８６ｈである。

【００４７】

直前のリードアクセスがエラーのとき、図３ｂの形式であり、アクセス結果３１２の値が８０ＸＸｈで、Ｌｅ３１３の値は０６ｈである。

【００４８】

アクセスエラー時にアクセス結果３１２（または３２２）に設定する８０ＸＸｈにおいて、エラー内容を示すコードＸＸの例を以下に示す。

【００４９】

ＸＸ＝０１は、指定されたレコード番号がアクセス可能な範囲外であるエラーを意味する。

【００５０】

ＸＸ＝０２は、フラッシュメモリチップ１３０が故障などにより利用できないエラーを意味する。

【００５１】

ＸＸ＝０３は、第１制御バイト３０１の下位４ビットが現在のアクセスモードに合致しないエラーを意味する。

【００５２】

ＸＸ＝０４は、第２制御バイト３０２で要求された次回のアクセスモードが不正であるエラーを意味する。

【００５３】

図４を参照しながら、ＩＣカードチップ１５０内のアプレットが、セキュアデータエリア１３３にアクセスを開始するときの処理の流れ、およびライト／リード転送コマンドによってそこに対するアクセスを実行するときの処理の流れを説明する。

【００５４】

ホスト機器１６０はMMC１１０にセキュアライトコマンドを発行し（４０１）、セキュアライトデータ６０１を入力する（４０２）。コントローラチップ１２０は、セキュアライトデータ６０１からＩＣカードコマンドのコマンドＡＰＤＵ６０２を抽出し（４０３）、それを用いてＩＣカードチップ１５０にＩＣカードコマンドを発行する（４０４）。

【００５５】

ＩＣカードチップ１５０は、そのＩＣカードコマンドを受信し（４０５）、セキュアデータエリア１３３へのアクセスを要求するＩＣカードレスポンス３００を作成し、それを返信する（４０６）。コントローラチップ１２０は、このレスポンスを受信し、そのＳＷ１バイト３０５とＳＷ２バイト３０６が９０ＦＦｈであるかを調べる（４０７）。９０ＦＦｈでないならばステップ４０８に移る。９０ＦＦｈであるならば、第１制御バイト３０１の上位４ビットが０００１（アクセス開始要求）であるかを調べる（４１２）。０００１でないならばステップ４２０に移る。０００１であるならば、管理テーブル１３６がロックされているか

[redacted]調べる（４１３）。アンロックされているならばステップ４０８に移る。ロックされているならば、後続出力データ３０３に含まれるＡＩＤで管理テーブル１３６上のＡＩＤ１３７を検索する（４１４）。一致するＡＩＤを検出したならば（４１５）、コントローラチップ１２０はアクセス開始要求を承認し、ステップ４１６に移る。検出しなければアクセス開始要求を却下し、ステップ４０８に移る。ステップ４１６では、検出したＡＩＤ１３７に対応するセキュアデータブロックを選択し、それをアクティブにする。さらに、対応する転送コマンドコード１３８を取得する（４１７）。そして、第１制御バイト３０１の下位４ビットを調べて、開始するアクセスモードを取得し（４１８）、そのアクセスモードに応じて図３ｂに示すようなライト／リード転送コマンドを作成する（４１９）。その後、ステップ４０４に戻り、ＩＣカードチップ１５０にライト／リード転送コマンドを発行する。

【００５６】

ステップ４２０では、第１制御バイト３０１の上位４ビットが００１０（アクセス実行要求）であるかを調べる。００１０でないならばステップ４０８に移る。００１０であるならば、アクティブなセキュアデータブロックが存在するか、また第１制御バイト３０１の下位４ビットがコントローラチップ１２０の認知するアクセスモードに合致するかを調べる（４２１）。いずれかが偽ならばステップ４０８に移る。両者とも真ならば、アクセス実行を承認し、後続出力データ３０３に含まれるレコード番号を取得する（４２２）。そして、そのレコード番号の指示するデータに対してライト／リードを実行する（４２３）。このとき、ライトモードの場合は、後続出力データ３０３に含まれる１２８バイトのデータをライトする。次に、そのアクセスの結果を示すコードを３１２または３２２に設定する（４２４）。そして、第１制御バイト３０１の下位４ビットを調べて、次回のアクセスモードを取得し（４１８）、そのアクセスモードに応じて図３ｂまたは図３ｃに示すようなライト／リード転送コマンドを作成する（４１９）。その後、ステップ４０４に戻り、ＩＣカードチップ１５０にライト／リード転送コマンドを発行する。

【００５７】

[redacted]ステップ４０８では、ＩＣカードチップ１５０が返信したレスポンスＡＰＤＵ６１２からセキュアリードデータ６１１を作成する。ステップ４０８に至ることによって、セキュアデータエリア１３３へのアクセスは終了する。この後、ホスト機器１６０はセキュアリードコマンドを発行し（４０９）、コントローラチップ１２０はセキュアリードデータ６１１を出力する（４１０）。そして、ホスト機器１６０はセキュアリードデータ６１１を受信する（４１１）。

【００５８】

以上より、ホスト機器１６０から一組のセキュアライト／セキュアリードコマンドをMMC１１０に処理させる間に、ＩＣカードチップ１５０内のアプレットは任意の回数、セキュアデータエリア１３３へアクセスすることができる。

【００５９】

以下、管理エリア１３２に関するアクセスについて説明する。

【００６０】

ホスト機器１６０が管理エリア１３２の情報にアクセスできるように、MMC１１０は、以下の４つの管理コマンドに応じることができる。すなわち、（１）アプレット登録コマンド、（２）アプレット登録解除コマンド、（３）管理テーブルロックコマンド、（４）管理テーブルアンロックコマンドの４つである。（１）は、管理テーブル１３６にセキュアデータエリア１３３を利用するアプレットを登録し、アプレットが利用するセキュアデータブロックを割り当てるコマンド、（２）は、管理テーブル１３６からアプレットの登録情報を削除し、セキュアデータブロックの割り当てを解除するコマンド、（３）は、管理テーブル１３６上の登録情報の変更を禁止するコマンド、（４）は、管理テーブル上１３６の登録情報の変更を許可するコマンドである。これらのコマンドは、一般のセキュリティ処理と同じくセキュアライトコマンドとセキュアリードコマンドのプロトコルによって実施され、コントローラチップ１２０によって処理される。また、その際に入出力されるセキュアライトデータとセキュアリードデータに含まれるＡＰＤＵ（図６における６０２や６１２）を利用して各処理（登録、登録解除、ロック、アンロック）に必要な情報を交換する。

【００６１】

[redacted]アプレット登録コマンドとアプレット登録解除コマンドでは、ＤａｔａＩｎ６０６にＡＩＤを設定する。このＡＩＤによって登録したいアプレットを指定する。ＡＩＤとセキュアデータブロックとをどのように対応付けるかはコントローラチップ１２０が決定する。ホスト機器１６０はセキュアデータブロックを直接指定できない。

【００６２】

管理テーブルロックコマンドでは、ＤａｔａＩｎ６０６に２５５バイトのパスワードを設定する。そのパスワードはパスワードエリア１３５に設定され、ロックフラグ１３４がＦＦｈ（ロック状態）になる。これにより、アプレット登録コマンドとアプレット登録解除コマンドが無効になる。すでにロック状態だった場合は、そのパスワードはパスワードエリア１３５に設定されず、アプレット登録コマンドとアプレット登録解除コマンドは有効のままとなる。

【００６３】

管理テーブルアンロックコマンドでは、ＤａｔａＩｎに２５５バイトのパスワードを設定する。そのパスワードはパスワードエリア１３５に設定された値と一致比較され、一致したならばロックフラグ１３４が００ｈ（アンロック状態）になる。これにより、アプレット登録コマンドとアプレット登録解除コマンドが有効になる。すでにアンロック状態だった場合は、アプレット登録コマンドとアプレット登録解除コマンドは無効のままとなる。

【００６４】

アプレット登録コマンドとアプレット登録解除コマンドが有効な状態（アンロック状態）では、パスワードを知らないホスト機器１６０によって管理テーブル１３６の情報が不正に変更され、あるアプレットが、それ自身がアクセス可能なセキュアデータブロック以外のセキュアデータブロックをライト／リードするという不正アクセスが発生しうる。そこで、コントローラチップ１２０は、ロックフラグ１３４の値が００ｈ（アンロック状態）では、ＩＣカードチップ１５０内で選択されているアプレットがセキュアデータエリアへアクセスするのを許可しない。ホスト機器１６０は、管理テーブル１３６の登録情報の設定／変更後は、管理テーブルロックコマンドにより必ずロックフラグ１３４をＦＦｈに設定しな

ければならない。

【００６５】

図５を参照しながら、上記４つの管理コマンドの処理の流れを説明する。

【００６６】

ホスト機器１６０はMMC１１０にセキュアライトコマンドを発行し（５０１）、セキュアライトデータ６０１を入力する（５０２）。コントローラチップ１２０は、セキュアライトデータ６０１からＩＣカードコマンドのコマンドＡＰＤＵ６０２を抽出し（５０３）、それが管理コマンドであるかを調べる（５０４）。管理コマンドならばステップ５０７に移る。一方、管理コマンドでないならば、そのコマンドＡＰＤＵ６０２を用いてＩＣカードチップ１５０にＩＣカードコマンドを発行し（５０５）、ＩＣカードチップ１５０からそのレスポンスを受信し（５０６）、ステップ５２７に移る。

【００６７】

ステップ５０７では、コントローラチップ１２０は、コマンドＡＰＤＵ６０２がアプレット登録コマンドを示すものかを調べる。アプレット登録コマンドならばステップ５１１に移る。さもなくば、それがアプレット登録解除コマンドを示すものかを調べる（５０８）。アプレット登録解除コマンドならばステップ５１２に移る。さもなくば、それが管理テーブルロックコマンドを示すものかを調べる（５０９）。管理テーブルロックコマンドならばステップ５１３に移る。さもなくば、それが管理テーブルアンロックコマンドを示すものかを調べる（５１０）。管理テーブルアンロックコマンドならばステップ５１４に移る。さもなくば、ステップ５２５に移る。

【００６８】

ステップ５１１では、ロックフラグ１３４を見て、管理テーブル１３６がアンロック状態かを調べる。ロック状態ならばステップ５２５に移る。アンロック状態ならば、ＤａｔａＩｎ６０６内のＡＩＤと同一のものが既に登録されているＡＩＤ１３７の中に存在するか調べる（５１５）。存在していればステップ５２５に移る。存在しなければ、管理テーブル１３６上に空きがあるか（つまり、まだ割り当てられていないセキュアデータブロックが存在するか）を調べる（５１６

）。空きがなければステップ５２５に移る。空きがあれば、そのセキュアデータブロックに対応するＡＩＤ１３７と転送コマンドコード１３８に、ＤａｔａＩｎ６０６に含まれるＡＩＤと転送コマンドコードを設定する（５１７）。これにより、ＡＩＤで示されたアプレットがそのセキュアデータブロックの利用権を獲得する。そして、ステップ５２６に移る。

【００６９】

ステップ５１２では、ロックフラグ１３４を見て、管理テーブル１３６がアンロック状態かを調べる。ロック状態ならばステップ５２５に移る。アンロック状態ならば、ＤａｔａＩｎ６０６内のＡＩＤで、登録されている全てのＡＩＤ１３７の中を検索する（５１８）。一致するＡＩＤを検出したならば（５１９）、管理テーブル１３６上からそのＡＩＤ１３７とそれに対応する転送コマンドコード１３８を削除する（５２０）。一致するＡＩＤを検出しなければステップ５２５に移る。これにより、ＡＩＤで示されたアプレットがそのセキュアデータブロックの利用権を失う。そして、ステップ５２６に移る。

ステップ５１３では、ロックフラグ１３４を見て、管理テーブル１３６がアンロック状態かを調べる。ロック状態ならばステップ５２５に移る。アンロック状態ならば、ロックフラグ１３４にＦＦｈを設定し（５２１）、管理テーブル１３６をロック状態にする。ＤａｔａＩｎ６０６内のパスワードをパスワードエリア１３５に設定する（５２２）。そして、ステップ５２６に移る。

【００７０】

ステップ５１４では、ロックフラグ１３４を見て、管理テーブル１３６がアンロック状態かを調べる。アンロック状態ならばステップ５２５に移る。ロック状態ならば、ＤａｔａＩｎ６０６内のパスワードがパスワードエリア１３５に設定したものと一致するかを調べる（５２３）。一致しないならば、ステップ５２５に移る。一致するならば、ロックフラグ１３４に００ｈを設定し（５２４）、管理テーブル１３６をアンロック状態にする。そして、ステップ５２６に移る。

【００７１】

ステップ５２５では、管理コマンドの処理でエラーが発生したことをホスト機器１６０に示すため、エラー内容を示すステータスコードを含むレスポンスＡＰ

ＤＵ６１２を作り、ステップ５２７に移る。ステップ５２６では、管理コマンドの処理が正常に終了したことをホスト機器１６０に示すため、正常終了（例えば、９０００ｈ）というステータスコードを含むレスポンスＡＰＤＵ６１２を作り、ステップ５２７に移る。

【００７２】

ステップ５２７では、レスポンスＡＰＤＵ６１２からセキュアリードデータ６１１を作成する。この後、ホスト機器１６０はセキュアリードコマンドを発行し（５２８）、コントローラチップ１２０はセキュアリードデータ６１１を出力する（５２９）。そして、ホスト機器１６０はセキュアリードデータ６１１を受信する（５３０）。

【００７３】

尚、本発明の適用に際しては、ＩＣカードチップ１５０がコントローラチップ１２０にセキュアデータエリア１３３へのアクセスを要求する手段として、ＳＷ１バイト３０５とＳＷ２バイト３０６に９０ＦＦｈという専用のステータス値を設定することを示したが、あくまでこれは一例であり、これ以外の手段でアクセスを要求してもよい。例えば、９０ＦＦｈ以外のステータスコードでもよいし、ＤａｔａＯｕｔ３０４内に専用のパスワード等を含ませてもよい。

【００７４】

尚、本発明の適用に際しては、ＭＭＣ１１０が、新たな（あるいは前記の）管理コマンドに応じて、セキュアデータエリア１３３のサイズを変化させることができる機能を有してもよい。また、新たな（あるいは前記の）管理コマンドに応じて、セキュアデータブロックの分割数（上述では分割数＝４）を変化させることができる機能を有してもよい。また、新たな（あるいは前記の）管理コマンドに応じて、各セキュアデータブロックのサイズを個別に変化させることができる機能を有してもよい。

【００７５】

尚、本発明の適用に際しては、上述のパスワードの長さは２５５バイトでなくてもよい。ただし、安全上、このパスワードは長いほうが好ましい。

【００７６】

尚、本発明の適用に際しては、アプレット登録解除コマンドで開放されたセキュアデータブロックに、それまでこのブロックを利用していたアプレットに関する機密データが残留し、次にそのブロックの使用権を得た他のアプレットがその機密データを取得する危険性がある。そこで、安全上、登録解除後に残留したデータを消去することが好ましい。その消去の実施は、上述のアプレット登録解除コマンドの処理中におこなってもよいし、ＭＭＣ１１０がホスト機器１６０からの新たな管理コマンドに応じておこなってもよい。

【００７７】

尚、本発明は、カード形式以外の記憶装置にも適用可能である。

【００７８】

【発明の効果】

本発明によれば、特定のアプリケーションプログラムに係る処理を実行する場合に、特定のアプリケーションプログラムに関係するデータをメモリ装置内部で処理することにより、特定のアプリケーションプログラムに係る処理の安全性を向上できるという効果を奏する。

【００７９】

本発明によれば、メモリ装置が実行すべきアプリケーションプログラムごとにメモリ装置内のメモリの異なるブロックを割り当てることにより、アプリケーションプログラム間のデータ干渉、即ち、あるアプリケーションプログラムに割り当てられたメモリが他のアプレットにもアクセスされてデータが侵害されることを抑制できるという効果を奏する。

【図面の簡単な説明】

【図１】本発明を適用したＭＭＣの内部構成を示す図である。

【図２】本発明を適用したＭＭＣの動作を概念的に示すフローチャートである。

【図３】コントローラチップとＩＣカードチップとの間のＩＣカードコマンドおよびＩＣカードレスポンスの構造を示す図である。

【図４】ＩＣカードチップからの要求に応じてフラッシュメモリチップ上のセキュアデータエリアに対するデータの読み書きを実行するフローチャートである。

【図５】ＩＣカードチップからの要求に応じてフラッシュメモリチップ上の管理

エリアに対するアプレットの登録およびその解除、また登録情報のロックおよびアンロックを実行するフローチャートである。

【図６】セキュアライトデータとセキュアリードデータの構成図である。

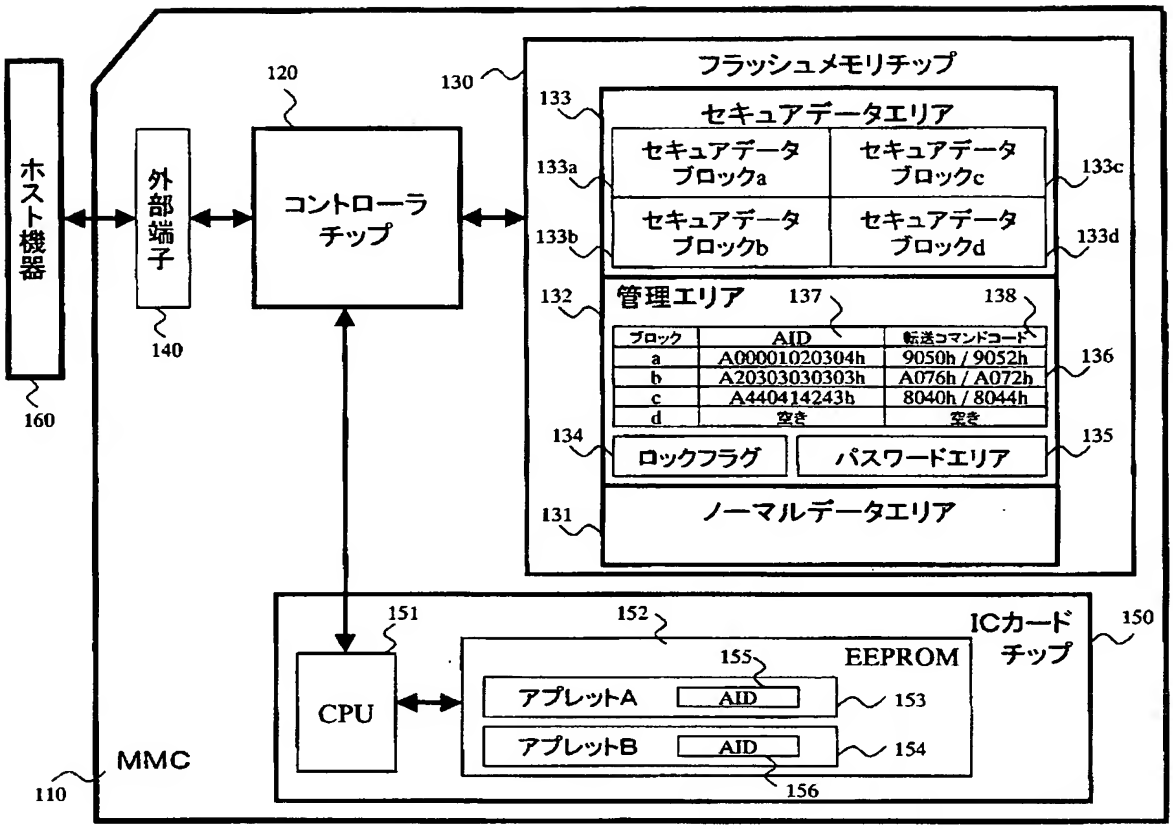
【符号の説明】

１１０…MMC、１２０…コントローラチップ、１３６…管理テーブル、１４０…MMC外部端子、１５０…ＩＣカードチップ、１６０…ホスト機器。

【書類名】図面

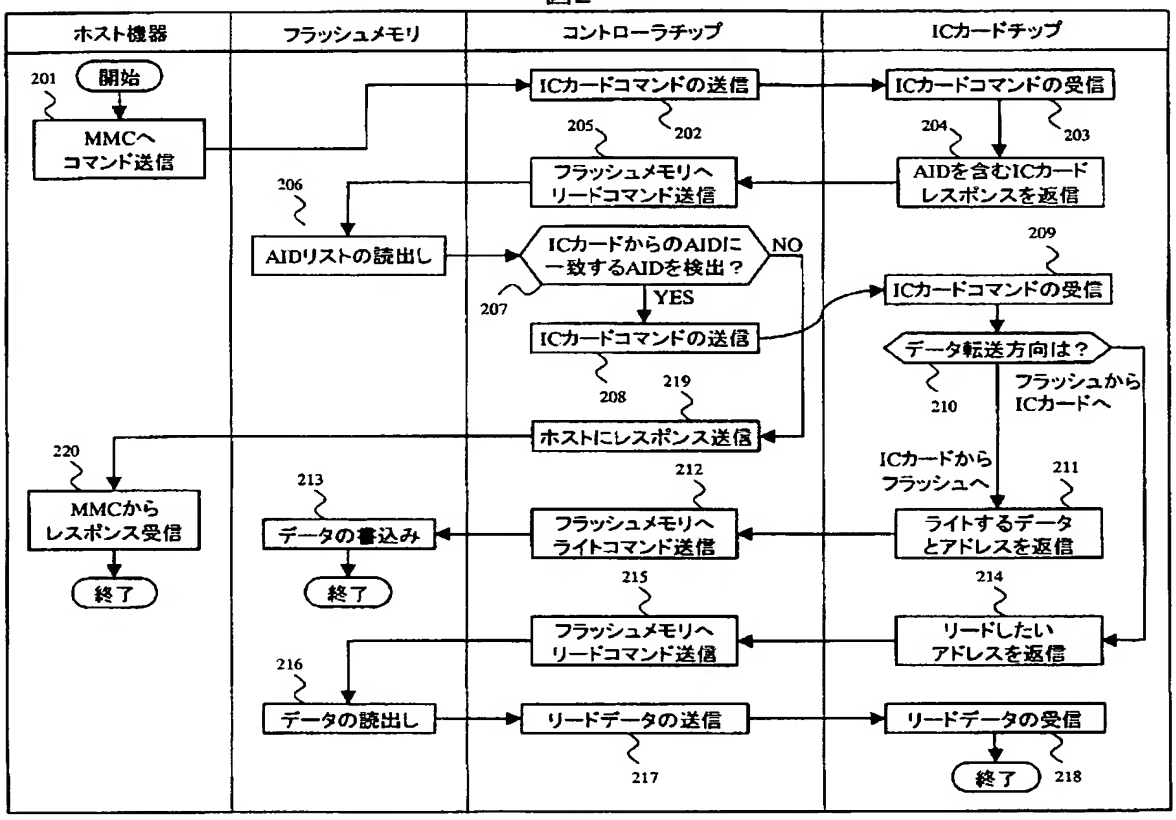
【図１】

図1


ホスト機器
160
外部端子
140
120
コントローラチップ
130
フラッシュメモリチップ
133
セキュアデータエリア
セキュアデータブロックa
セキュアデータブロックc
セキュアデータブロックb
セキュアデータブロックd
133a
133c
133b
133d
132
管理エリア
137
138
ブロック
AID
転送コマンドコード
a
A00001020304h
9050h / 9052h
b
A20303030303h
A076h / A072h
c
A440414243h
8040h / 8044h
d
空き
空き
136
134
ロックフラグ
パスワードエリア
135
131
ノーマルデータエリア
151
152
ICカードチップ
150
155
EEPROM
CPU
アプレットA
AID
153
アプレットB
AID
154
156
MMC
110

【図２】

図2


ホスト機器
フラッシュメモリ
コントローラチップ
ICカードチップ
201
開始
MMCへ
コマンド送信
ICカードコマンドの送信
202
ICカードコマンドの受信
203
205
フラッシュメモリへ
リードコマンド送信
204
AIDを含むICカード
レスポンスを返信
206
AIDリストの読出し
ICカードからのAIDに
一致するAIDを検出？
NO
YES
207
209
ICカードコマンドの受信
ICカードコマンドの送信
データ転送方向は？
208
210
フラッシュから
ICカードへ
219
ホストにレスポンス送信
220
ICカードから
フラッシュへ
212
211
213
MMCから
レスポンス受信
データの書込み
フラッシュメモリへ
ライトコマンド送信
ライトするデータ
とアドレスを返信
終了
終了
215
214
フラッシュメモリへ
リードコマンド送信
リードしたい
アドレスを返信
216
データの読出し
リードデータの送信
リードデータの受信
217
終了
218

【図３】

図3

図3a

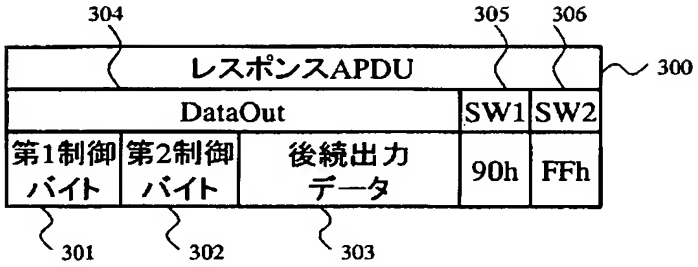


図3b

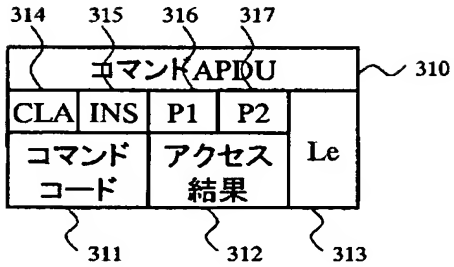
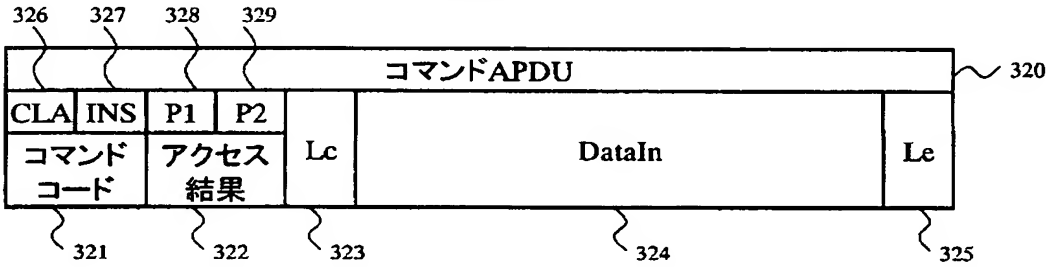
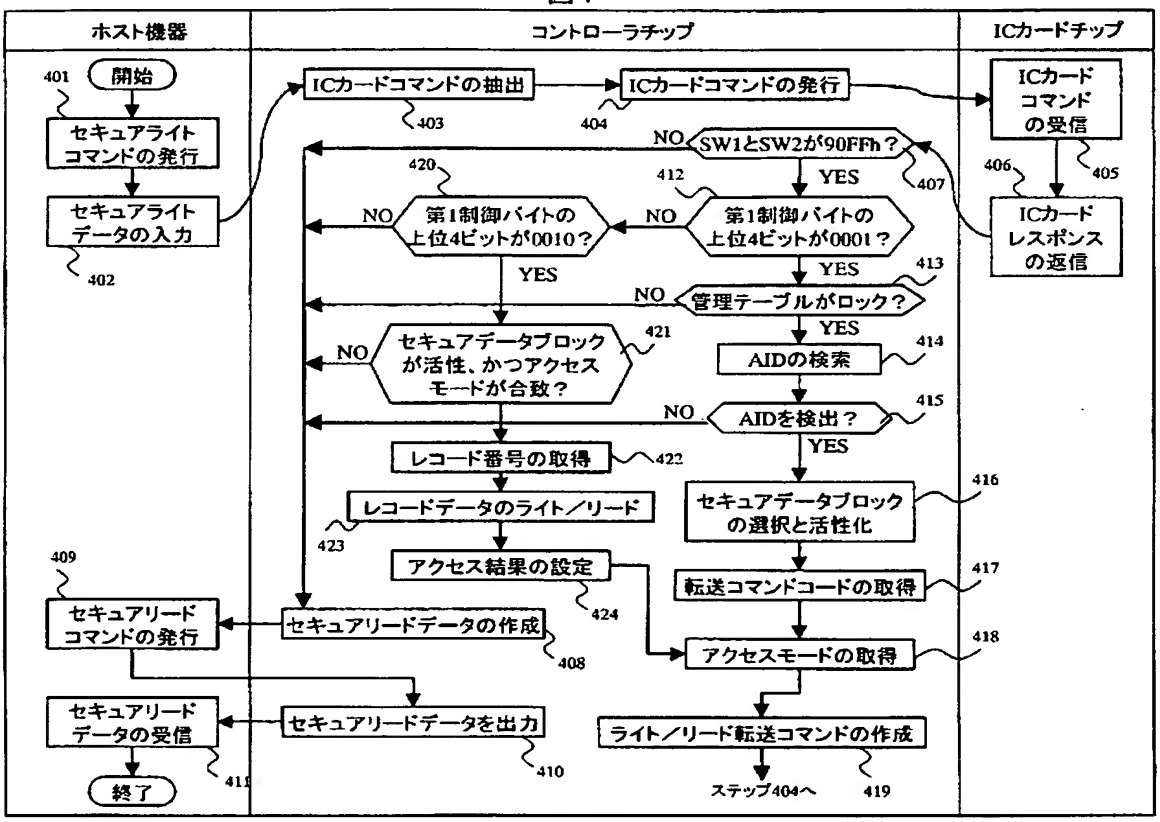


図3c



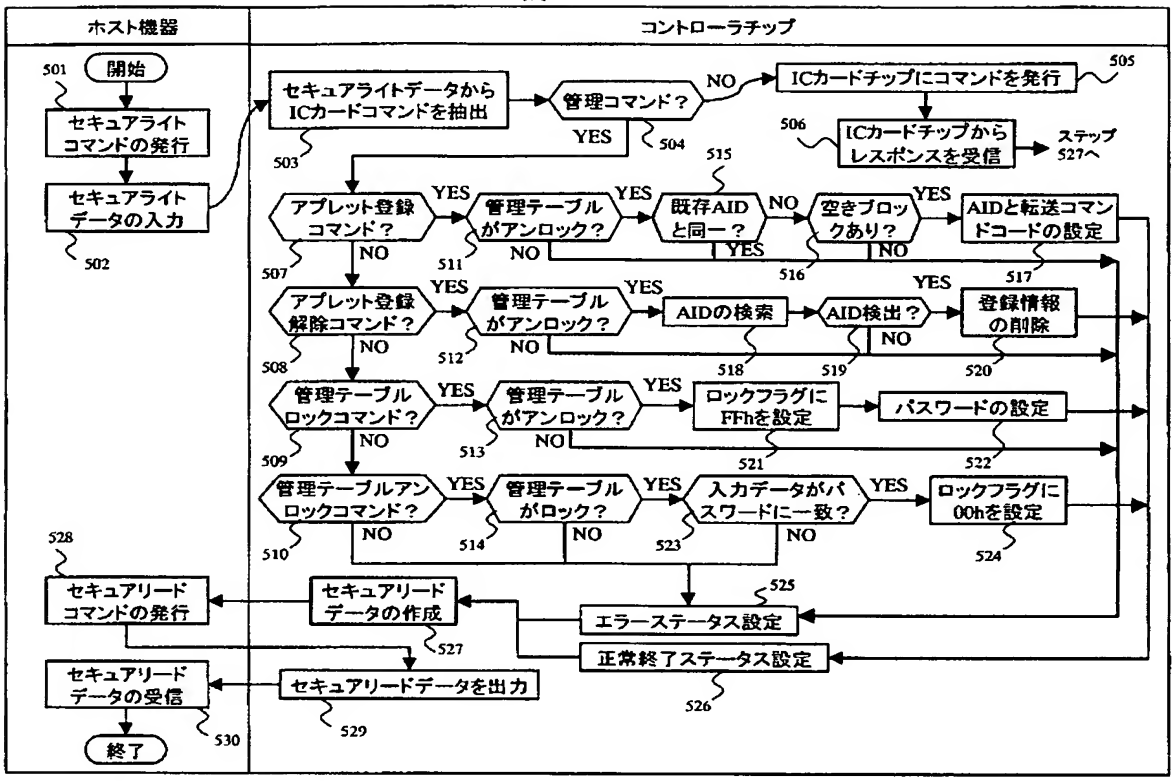
【図４】

図4


ホスト機器
コントローラチップ
ICカードチップ
401
開始
セキュアライトコマンドの発行
セキュアライトデータの入力
402
ICカードコマンドの抽出
403
ICカードコマンドの発行
404
ICカードコマンドの受信
405
406
ICカードレスポンスの返信
NO
SW1とSW2が90FFh？
407
YES
412
第1制御バイトの上位4ビットが0001？
NO
420
第1制御バイトの上位4ビットが0010？
NO
YES
413
管理テーブルがロック？
NO
YES
414
AIDの検索
421
セキュアデータブロックが活性、かつアクセスモードが合致？
NO
415
AIDを検出？
NO
YES
422
レコード番号の取得
416
セキュアデータブロックの選択と活性化
423
レコードデータのライト／リード
424
アクセス結果の設定
417
転送コマンドコードの取得
409
セキュアリードコマンドの発行
408
セキュアリードデータの作成
418
アクセスモードの取得
セキュアリードデータの受信
411
終了
410
セキュアリードデータを出力
ライト／リード転送コマンドの作成
ステップ404へ
419

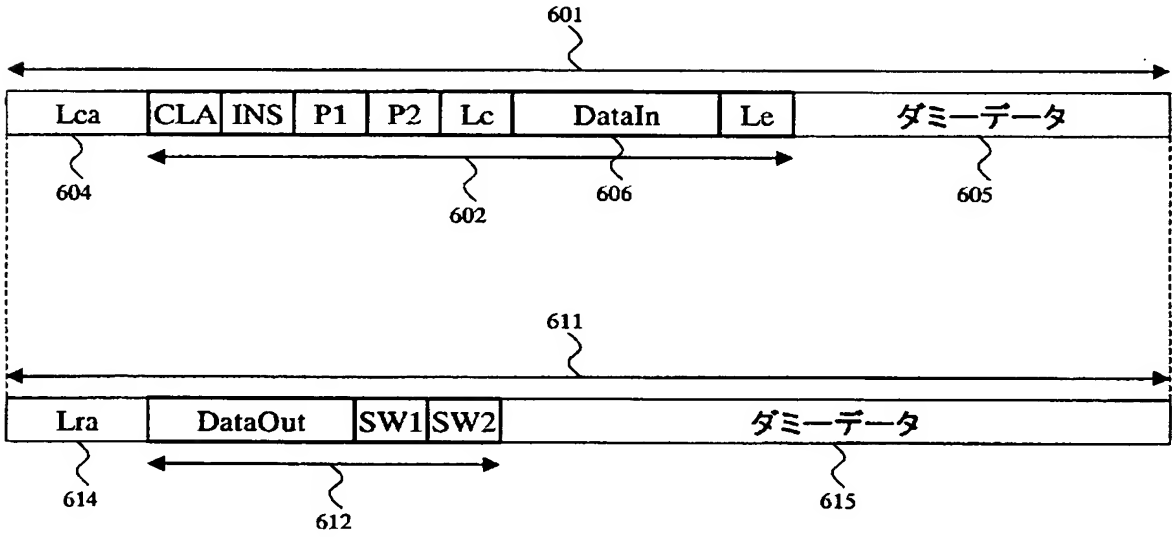
【図５】

図5


ホスト機器
コントローラチップ
開始
セキュアライトコマンドの発行
セキュアライトデータの入力
セキュアライトデータからICカードコマンドを抽出
管理コマンド？
ICカードチップにコマンドを発行
ICカードチップからレスポンスを受信
ステップ527へ
アプレット登録コマンド？
管理テーブルがアンロック？
既存AIDと同一？
空きブロックあり？
AIDと転送コマンドコードの設定
アプレット登録解除コマンド？
AIDの検索
AID検出？
登録情報の削除
管理テーブルロックコマンド？
ロックフラグにFFhを設定
パスワードの設定
管理テーブルアンロックコマンド？
管理テーブルがロック？
入力データがパスワードに一致？
ロックフラグに00hを設定
エラーステータス設定
正常終了ステータス設定
セキュアリードコマンドの発行
セキュアリードデータの作成
セキュアリードデータの受信
セキュアリードデータを出力
終了
YES
NO

【図６】

図6


601
Lca
CLA
INS
P1
P2
Lc
DataIn
Le
ダミーデータ
604
602
606
605
611
Lra
DataOut
SW1
SW2
ダミーデータ
614
612
615

【書類名】　要約書

【要約】

【課題】

ＩＣカードチップのアプレット間のデータ干渉、即ち、一のアプレットに割り当てられたメモリが他のアプレットにもアクセスされてデータが侵害されることを抑制する。

【解決手段】

本発明は、フラッシュメモリチップ１３０と、ＩＣカードチップ１５０と、ホストからの要求に応じてフラッシュメモリチップ及びＩＣカードチップへのデータの読み書きを制御するコントローラチップ１２０とを備え、フラッシュメモリチップは、ホスト機器からのデータを記憶するためのノーマルデータエリア１３１とＩＣカードチップからのデータを記憶するためのセキュアデータエリア１３３を有し、さらに、セキュアデータエリア１３３は、アプレット１５３，１５４ごとに割り当てられたセキュアデータブロック１３３ａ，１３３ｂ，１３３ｃ，１３３ｄに分割される。

【選択図】図１

認定・付加情報

特許出願の番号	特願２００３－０５０２４３
受付番号	５０３００３１３９３１
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　３月　４日

＜認定情報・付加情報＞

【提出日】　平成15年 2月27日

次頁無

【書類名】　出願人名義変更届（一般承継）

【あて先】　特許庁長官　殿

【事件の表示】

【出願番号】　特願2003- 50243

【承継人】

【識別番号】　503121103

【氏名又は名称】　株式会社ルネサステクノロジ

【承継人代理人】

【識別番号】　100080001

【弁理士】

【氏名又は名称】　筒井　大和

【提出物件の目録】

【包括委任状番号】　0308729

【物件名】　承継人であることを証明する登記簿謄本　1

【援用の表示】　特許第３１５４５４２号　平成１５年４月１１日付け提出の会社分割による特許権移転登録申請書　を援用する

【物件名】　権利の承継を証明する承継証明書　1

【援用の表示】　特願平１－２５１８８９号　同日提出の出願人名義変更届（一般承継）を援用する

【プルーフの要否】　要

認定・付加情報

特許出願の番号	特願２００３－０５０２４３
受付番号	５０３０１４０３５３５
書類名	出願人名義変更届（一般承継）
担当官	土井　恵子　　４２６４
作成日	平成１５年１１月　４日

＜認定情報・付加情報＞

【提出日】　平成15年 8月26日

特願２００３－０５０２４３

出　願　人　履　歴　情　報

識別番号　　[０００００５１０８]

１．変更年月日　　１９９０年　８月３１日
[変更理由]　　新規登録
住　所　　東京都千代田区神田駿河台４丁目６番地
氏　名　　株式会社日立製作所

特願２００３－０５０２４３

出　願　人　履　歴　情　報

識別番号　［５０３１２１１０３］

１．変更年月日　２００３年　４月　１日
［変更理由］　新規登録
住　所　東京都千代田区丸の内二丁目４番１号
氏　名　株式会社ルネサステクノロジ